Embedded Flash on a CMOS Process Enables Secure Hardware Encyrption on Deep Submicron Designs

Joel Rosenberg
Sr. Product Line Director
Virage Logic Corporation
(510) 360-8096
joel.rosenberg@viragelogic.com

Design and applications security along with intellectual property protection and digital rights management are a critical issue in today's advanced electronics systems design. In a typical system design user data is loaded from an external memory into a system-on-chip (SOC) upon system power up. Anytime data crosses either internal or external pin boundaries it is vulnerable to theft. A probe can be placed on the data line compromising the security of the data. Encryption algorithms typically require between 256 - 1K bits of embedded non-volatile memory for storing the encryption key. Hence it is desirable to embed the NVM into the SOC to make the data "secure". A key design challenge associated with deploying Flash technology is that Flash is usually manufactured on a "lagging edge", .25u or older process which is not compatible with today's more advanced, deep submicron 0.18, .13 and 90 nm processes. Embedded flash is becoming available on 0.18u today, but requires many additional mask and process steps, adding significant complexity and cost to the entire SOC, especially if only a few bits are required for security.

This paper will discuss an embedded in-system reprogrammable NVM technology which solves this problem by providing small amounts of embedded NVM on a completely standard CMOS logic process requiring no additional mask or process steps. This solution is more optimized for hardware encryption than external memory, electrical fuses (eFuse) or laser fuse technology in that it utilizes a single poly floating gate (Flash) technology that makes it impossible to visually identify the state of the encryption bits or data as it crosses pin boundaries inside or outside a packaged IC. This solution is ideal for embedding encryption keys for security in wireless networks, digital rights management in consumer recording electronics, and replacing laser fuses for silicon repair. In addition, this capability provides an ideal solution for embedded ROM applications that require the flexibility of Flash without the added cost. A small amount of this embedded NVM can be added to provide "patch code" capability or for other purposes.

This paper will explain the requirements for providing embedded reprogrammable NVM into SOCs manufactured on advanced processes and discuss the ways that it can be deployed to enable design and applications security without increase complexity or cost.